PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-233771
(43)Date of publication of application : 02.09.1998

(51)Int.Cl. H04L 9/32
G09C 1/00

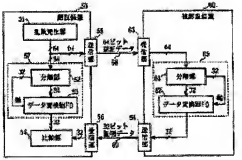
(21)Application number : 09-296515
(22)Date of filing : 29.10.1997

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
TOSHIBA CORP
(72)Inventor : TATEBAYASHI MAKOTO
MATSUZAKI NATSUME
HIRAYAMA KOICHI

(30)Priority
Priority number : 08290375 Priority date : 31.10.1996 Priority country : JP

(54) UNIDIRECTIONAL DATA CONVERSION DEVICE AND DEVICE AUTHENTICATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To execute authentication through the use of authentication data whose length is twice as much as a conventional one without increasing a circuit scale by converting first separation data based on conversion algorithm where second separation data is set to be a key and generating output data.
SOLUTION: In an authentication device 50, a separation part 52 separates the random number of 64 bits into two pieces of separation data of 64 bits. A data converter 53 converts one separation data with other separation data as the key. In a device to be verified 60, a separation part 61 separates authentication data of 64 bits into two pieces of separation data of 32 bits. A data converter 62 converts one separation data with other separation data as the key and returns it to the verification device 50. The comparison part 54 of the authentication device 50 compares two pieces of data of 32 bits, which are outputted from the data converters 53 and 62 in both devices 50 and 60. When they are matched, the authentication device 50 verifies that the device to be verified 60 is a just unit.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－233771

(43)公開日　平成10年(1998)９月２日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ａ
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｅ

審査請求　未請求　請求項の数25　ＯＬ　（全 16 頁）

(21)出願番号　特願平9－296515

(22)出願日　平成９年(1997)10月29日

(31)優先権主張番号　特願平8－290375

(32)優先日　平８(1996)10月31日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　館林　誠
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　松崎　なつめ
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　弁理士　中島　司朗

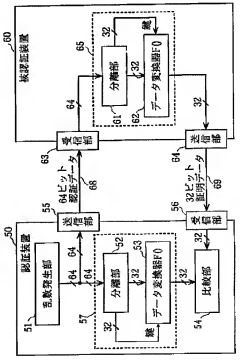
最終頁に続く

(54)【発明の名称】　一方向データ変換装置及び機器認証システム

(57)【要約】

【課題】　回路規模を大幅に増大することなく従来の２倍長の認証データを用いて認証を行うことができる安全性の高い機器認証システムを提供する。

【解決手段】　認証装置５０は、６４ビットの乱数を発生する乱数発生部５１と、その乱数を認証データとして被認証装置６０に送信する送信部５５と、その乱数を２個の３２ビットデータに分離する分離部５２と、分離された一方のデータに対して、他方のデータを鍵とする秘密のアルゴリズムに基づいて変換するデータ変換器５３と、送信した認証データに対して被認証装置６０から返信されてきた３２ビットの証明データを受信する受信部５６と、その証明データとデータ変換器５３からの出力データとが一致するか否かを判断する比較部５４とを備え、被認証装置６０も、認証装置５０が備える分離部５２及びデータ変換器５３と同一機能の分離部６１及びデータ変換器６２を備える。



1

【特許請求の範囲】

【請求項１】　２ｎビットの入力データをｎビットの出力データに変換する一方向データ変換装置であって、

前記入力データをその入力データの相異なる桁位置のｎビットずつに分離することにより、ｎビットの第１分離データとｎビットの第２分離データを生成する分離手段と、

前記第１分離データに対して前記第２分離データを鍵とする変換アルゴリズムに基づいて変換することにより、前記出力データを生成するデータ変換手段とを備えることを特徴とする一方向データ変換装置。

【請求項２】　前記一方向データ変換装置はさらに、

ｎビットの秘密鍵を記憶する秘密鍵記憶手段と、

前記分離手段から生成された第２分離データを用いて前記秘密鍵を変更することにより、ｎビットの変更鍵を生成する秘密鍵変更手段とを備え、

前記データ変換手段は、前記第２分離データに代えて前記変更鍵を鍵とする前記変換アルゴリズムに基づいて前記第１分離データを変換することを特徴とする請求項１記載の一方向データ変換装置。

【請求項３】　前記データ変換手段による変換は、一方向性変換であることを特徴とする請求項２記載の一方向データ変換装置。

【請求項４】　伝送路で接続された認証装置と被認証装置からなる機器認証システムであって、

前記認証装置は、

２ｎビットの乱数を発生する乱数発生手段と、

前記乱数を認証データとして前記被認証装置に送信する送信手段と、

前記乱数を入力データとし、秘密のアルゴリズムに基づいてｎビットの出力データに変換する一方向データ変換手段と、

前記認証データに対して被認証装置から返信されてきたｎビットの証明データを受信する受信手段と、

前記出力データと前記証明データとが一致するか否かを判断する比較手段とを備え、

前記被認証装置は、

前記認証装置から送信されてきた認証データを受信する受信手段と、

前記認証データを入力データとし、前記アルゴリズムと同一の秘密のアルゴリズムに基づいてｎビットの出力データに変換する一方向データ変換手段と、

前記出力データを前記認証データに対する証明データとして前記認証装置に返信する送信手段とを備えることを特徴とする機器認証システム。

【請求項５】　前記認証装置及び前記被認証装置の一方向データ変換手段は、いずれも、

前記入力データをその入力データの相異なる桁位置のｎビットずつに分離することにより、ｎビットの第１分離データとｎビットの第２分離データを生成する分離手段

2

と、

前記第１分離データに対して前記第２分離データを鍵とする変換アルゴリズムに基づいて変換することにより、前記出力データを生成するデータ変換手段とを有することを特徴とする請求項４記載の機器認証システム。

【請求項６】　前記認証装置及び前記被認証装置の一方向データ変換手段は、いずれもさらに、

ｎビットの秘密鍵を記憶する秘密鍵記憶手段と、

前記分離手段から生成された第２分離データを用いて前記秘密鍵を変更することにより、ｎビットの変更鍵を生成する秘密鍵変更手段とを有し、

前記認証装置及び前記被認証装置のデータ変換手段は、前記第２分離データに代えて前記変更鍵を鍵とする前記変換アルゴリズムに基づいて前記第１分離データを変換することを特徴とする請求項５記載の機器認証システム。

【請求項７】　前記認証装置及び前記被認証装置のデータ変換手段による変換は、いずれも一方向性変換であることを特徴とする請求項６記載の機器認証システム。

【請求項８】　伝送路で接続された認証装置と被認証装置からなる機器認証システムにおける認証装置であって、

２ｎビットの乱数を発生する乱数発生手段と、

前記乱数を認証データとして前記被認証装置に送信する送信手段と、

前記乱数を入力データとし、秘密のアルゴリズムに基づいてｎビットの出力データに変換する一方向データ変換手段と、

前記認証データに対して被認証装置から返信されてきたｎビットの証明データを受信する受信手段と、

前記出力データと前記証明データとが一致するか否かを判断する比較手段とを備えることを特徴とする認証装置。

【請求項９】　前記一方向データ変換手段は、

前記入力データをその入力データの相異なる桁位置のｎビットずつに分離することにより、ｎビットの第１分離データとｎビットの第２分離データを生成する分離手段と、

前記第１分離データに対して前記第２分離データを鍵とする変換アルゴリズムに基づいて変換することにより、前記出力データを生成するデータ変換手段とを有することを特徴とする請求項８記載の認証装置。

【請求項１０】　前記一方向データ変換手段はさらに、

ｎビットの秘密鍵を記憶する秘密鍵記憶手段と、

前記分離手段から生成された第２分離データを用いて前記秘密鍵を変更することにより、ｎビットの変更鍵を生成する秘密鍵変更手段とを有し、

前記データ変換手段は、前記第２分離データに代えて前記変更鍵を鍵とする前記変換アルゴリズムに基づいて前記第１分離データを変換することを特徴とする請求項９

記載の認証装置。

【請求項１１】　前記データ変換手段による変換は、一方向性変換であることを特徴とする請求項１０記載の認証装置。

【請求項１２】　前記認証装置はさらに、

光ディスクからデジタル著作物を読み出す光ディスク読み出し手段と、

前記比較手段によって一致すると判断された場合に、前記デジタル著作物を前記被認証装置に転送するデータ転送手段とを備えることを特徴とする請求項１１記載の認証装置。

【請求項１３】　伝送路で接続された認証装置と被認証装置からなる機器認証システムにおける被認証装置であって、

前記認証装置から送信されてきた２ｎビットの認証データを受信する受信手段と、

前記認証データを入力データとし、秘密のアルゴリズムに基づいてｎビットの出力データに変換する一方向データ変換手段と、

前記出力データを前記認証データに対する証明データとして前記認証装置に返信する送信手段とを備えることを特徴とする被認証装置。

【請求項１４】　前記一方向データ変換手段は、

前記入力データをその入力データの相異なる桁位置のｎビットずつに分離することにより、ｎビットの第１分離データとｎビットの第２分離データを生成する分離手段と、

前記第１分離データに対して前記第２分離データを鍵とする変換アルゴリズムに基づいて変換することにより、前記出力データを生成するデータ変換手段とを有することを特徴とする請求項１３記載の被認証装置。

【請求項１５】　前記一方向データ変換手段はさらに、

ｎビットの秘密鍵を記憶する秘密鍵記憶手段と、

前記分離手段から生成された第２分離データを用いて前記秘密鍵を変更することにより、ｎビットの変更鍵を生成する秘密鍵変更手段とを有し、

前記データ変換手段は、前記第２分離データに代えて前記変更鍵を鍵とする前記変換アルゴリズムに基づいて前記第１分離データを変換することを特徴とする請求項１４記載の被認証装置。

【請求項１６】　前記データ変換手段による変換は、一方向性変換であることを特徴とする請求項１５記載の被認証装置。

【請求項１７】　前記被認証装置はさらに、

前記認証装置から転送されてきたデジタル著作物を受信する転送データ受信手段と、

受信したデジタル著作物を映像再生する映像再生手段とを備えることを特徴とする請求項１６記載の被認証装置。

【請求項１８】　伝送路で接続された認証装置と被認証

装置からなる機器認証システムであって、

前記認証装置は、

２ｎビットの乱数を発生する乱数発生手段と、

前記乱数をその乱数の相異なる桁位置のｎビットずつに分離することにより、ｎビットの第１分離データとｎビットの第２分離データを生成する分離手段と、

前記第１分離データに対して前記第２分離データを暗号鍵とする暗号アルゴリズムに基づいて暗号化することにより、ｎビットの暗号文を生成する暗号化手段と、

前記暗号文と前記第２分離データとを各ビットを混ぜることで結合し、２ｎビットの出力データを生成する結合手段と、

前記出力データを認証データとして前記被認証装置に送信する送信手段と、

前記認証データに対して被認証装置から返信されてきたｎビットの証明データを受信する受信手段と、

前記証明データと前記第１分離データとが一致するか否かを判断する比較手段とを備え、

前記被認証装置は、

前記認証装置から送信されてきた認証データを受信する受信手段と、

受信した認証データをその認証データの相異なる桁位置のｎビットずつに分離することにより、前記暗号文と同じｎビットの第３分離データと前記第２分離データと同じｎビットの第４分離データを生成する分離手段と、

前記第３分離データに対して前記第４分離データを復号鍵とする復号アルゴリズムに基づいて復号化することにより、ｎビットの復号文を生成する復号化手段と、

前記復号文を前記認証データに対する証明データとして前記認証装置に返信する送信手段とを備えることを特徴とする機器認証システム。

【請求項１９】　前記認証装置はさらに、

ｎビットの秘密鍵を記憶する秘密鍵記憶手段と、

前記分離手段から生成された第２分離データを用いて前記秘密鍵を変更することにより、ｎビットの変更鍵を生成する秘密鍵変更手段とを備え、

前記暗号化手段は、前記第２分離データに代えて前記変更鍵を暗号鍵とする前記暗号アルゴリズムに基づいて前記第１分離データを暗号化し、

前記被認証装置はさらに、

ｎビットの秘密鍵を記憶する秘密鍵記憶手段と、

前記分離手段から生成された第４分離データを用いて前記秘密鍵を変更することにより、ｎビットの変更鍵を生成する秘密鍵変更手段とを備え、

前記復号化手段は、前記第４分離データに代えて前記変更鍵を復号鍵とする前記復号アルゴリズムに基づいて前記第３分離データを復号化することを特徴とする請求項１８記載の機器認証システム。

【請求項２０】　伝送路で接続された認証装置と被認証装置からなる機器認証システムにおける認証装置であっ

て、
２ｎビットの乱数を発生する乱数発生手段と、
前記乱数をその乱数の相異なる桁位置のｎビットずつに分離することにより、ｎビットの第１分離データとｎビットの第２分離データを生成する分離手段と、
前記第１分離データに対して前記第２分離データを暗号鍵とする暗号アルゴリズムに基づいて暗号化することにより、ｎビットの暗号文を生成する暗号化手段と、
前記暗号文と前記第２分離データとを各ビットを混ぜることで結合し、２ｎビットの出力データを生成する結合手段と、
前記出力データを認証データとして前記被認証装置に送信する送信手段と、
前記認証データに対して被認証装置から返信されてきたｎビットの証明データを受信する受信手段と、
前記証明データと前記第１分離データとが一致するか否かを判断する比較手段と
を備えることを特徴とする認証装置。
【請求項２１】　前記認証装置はさらに、
ｎビットの秘密鍵を記憶する秘密鍵記憶手段と、
前記分離手段から生成された第２分離データを用いて前記秘密鍵を変更することにより、ｎビットの変更鍵を生成する秘密鍵変更手段とを備え、
前記暗号化手段は、前記第２分離データに代えて前記変更鍵を暗号鍵とする前記暗号アルゴリズムに基づいて前記第１分離データを暗号化することを特徴とする請求項２０記載の認証装置。
【請求項２２】　前記認証装置はさらに、
光ディスクからデジタル著作物を読み出す光ディスク読み出し手段と、
前記比較手段によって一致すると判断された場合に、前記デジタル著作物を前記被認証装置に転送するデータ転送手段とを備えることを特徴とする請求項２１記載の認証装置。
【請求項２３】　伝送路で接続された認証装置と被認証装置からなる機器認証システムにおける被認証装置であって、
前記認証装置から送信されてきた２ｎビットの認証データを受信する受信手段と、
受信した認証データをその認証データの相異なる桁位置のｎビットずつに分離することにより、ｎビットの第１分離データとｎビットの第２分離データを生成する分離手段と、
前記第１分離データに対して前記第２分離データを復号鍵とする復号アルゴリズムに基づいて復号化することにより、ｎビットの復号文を生成する復号化手段と、
前記復号文を前記認証データに対する証明データとして前記認証装置に返信する送信手段とを備えることを特徴とする被認証装置。
【請求項２４】　前記被認証装置はさらに、
ｎビットの秘密鍵を記憶する秘密鍵記憶手段と、
前記分離手段から生成された第２分離データを用いて前記秘密鍵を変更することにより、ｎビットの変更鍵を生成する秘密鍵変更手段とを備え、
前記復号化手段は、前記第２分離データに代えて前記変更鍵を復号鍵とする前記復号アルゴリズムに基づいて前記第１分離データを復号化することを特徴とする請求項２３記載の被認証装置。
【請求項２５】　前記被認証装置はさらに、
前記認証装置から転送されてきたデジタル著作物を受信する転送データ受信手段と、
受信したデジタル著作物を映像再生する映像再生手段とを備えることを特徴とする請求項２４記載の被認証装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、一方向データ変換装置及びそれを用いた機器認証システムに関し、特に、大きなサイズの伝送データを用いて認証する技術に関する。
【０００２】
【従来の技術】ディジタル化された文書、音声、画像、プログラムなどのデータをネットワークを介して通信を行うシステムや、前記ディジタルデータを記録保存、読み出しするシステム等においては、前記ディジタルデータにアクセスしようとする者が予め許可された正当な者かどうかを事前に検査する必要がある。
【０００３】そのために、ネットワークや記録媒体へのデータアクセスに際しては、アクセスの正当性を示すために認証手続きが用いられている。最も簡単な認証方式として、アクセス者からＩＤとパスワードを送る方式がある。しかし、この方式では、伝送路を流れる他人のＩＤとパスワードを盗聴等によって入手すれば簡単に不正な認証を行うことができるので、安全性が高いとは言えない。
【０００４】安全性の高い従来の機器認証システムとして、一方向性関数を用いる第１の従来技術と、暗号器と復号器の対を用いる第２の従来技術がある。図１５は、一方向性関数を用いた第１の従来技術に係る機器認証システムの構成を示すブロック図である。このシステムは、伝送路２４、２５を介して接続された認証装置１０と被認証装置２０から構成される。
【０００５】認証装置１０は、被認証装置２０を認証する側の機器であり、３２ビットの乱数を発生する乱数発生部１１と、その乱数を認証データとして被認証装置２０に送信する送信部１４と、その乱数を秘密の一方向性関数ｆ()に基づいて変換するデータ変換器１２と、被認証装置２０から証明データを受信する受信部１５と、その証明データとデータ変換器１２が生成したデータとの一致を比較する比較部１３とから構成される。なお、認

証データとは、認証装置から被認証装置に送られるチャレンジデータであって、認証装置が被認証装置に対して自己の正当性を証明させる機会を与えるためのデータをいう。

【０００６】一方、被認証装置２０は、認証装置１０に対して自己の正当性を証明する機器であり、認証装置１０から送られてきた認証データを受信する受信部２２と、その認証データを秘密の一方向性関数ｆ()に基づいて変換するデータ変換器２１と、データ変換器２１が生成したデータを証明データとして認証装置１０に返信する送信部２３とから構成される。なお、証明データとは、認証データを受信した被認証装置が自己の正当性を証明するために認証装置に返信するレスポンスデータをいう。

【０００７】本図では、認証装置１０が備えるデータ変換器１２と被認証装置２０が備えるデータ変換器２１は同一である（同一の関数ｆ()に基づく変換を行う）ので、乱数発生部１１が発生した１個の乱数に対して、認証装置１０及び被認証装置２０は同一の変換を行うことから、比較部１３での比較結果は一致することになる。これによって、認証装置１０は「相手機器（被認証装置２０）は自己が備える秘密のデータ変換器１２と同一のデータ変換器を備える」と判断し、被認証装置２０の正当性を認める（認証する）。

【０００８】一方、比較部１３での比較結果が不一致となる場合は、認証装置１０は、「相手機器は自己が備える秘密のデータ変換器１２と同一のデータ変換器を備えない」ことを知るので、相手機器の正当性を認めない（認証しない）。なお、本システムにおいて、乱数により認証の都度異なる認証データを用いるのは、次の理由による。

【０００９】もし毎回固定の認証データを用いる場合には、それに対する毎回固定の証明データは伝送路２５を一度盗聴するだけで第３者が入手可能であり、それを用いて不正な被認証装置が正当な被認証装置を装って認証させてしまうことが出来るからである。図１６は、暗号器と復号器の対を用いた第２の従来技術に係る機器認証システムの構成を示すブロック図である。

【００１０】第１の従来技術では、両装置１０、２０それぞれは同一のデータ変換器１２、２１を備えたが、この第２の従来技術では、両装置３０、４０それぞれは秘密の暗号アルゴリズムＥ()に基づく暗号化をする暗号器３２、その暗号アルゴリズムＥ()の逆変換である秘密の復号アルゴリズムＤ()に基づく復号化をする復号器４１を備える。また、第１の従来技術では、認証データは乱数そのものであり、認証装置１０は両データ変換器１２、２１の変換結果どうしを比較したが、この第２の従来技術では、認証装置３０が送信する認証データは乱数を暗号化した暗号文であり、認証装置３０は、証明データとして被認証装置４０から返信される復号文と暗号化前の元の乱数とを比較する。

【００１１】この第２の従来技術においても、比較部３３での比較結果が一致した場合に、認証装置３０は「相手機器（被認証装置４０）は自己が備える秘密の暗号器３２に対応する復号器４１を備える」と判断し、被認証装置４０の正当性を認める（認証する）ことができる。ところで、このような従来の機器認証システムでは、認証データとそれに対応する証明データとの組合せの種類（組数）は充分に大きいことが必要とされる。

【００１２】もし、不正な第３者による伝送路２４、２５、４４、４５の盗聴によって、認証データとそれに対応する正しい証明データとの組が全ての組合せについて収集され尽くされた場合には、もはや秘密のアルゴリズムｆ()、Ｅ()、Ｄ()自体が解読されたことに等しいからである。また、不正な機器が認証装置になりすまして、全てのとり得る認証データを順次に正当な被認証装置に送信し、それぞれに対する証明データを収集するという不正行為に対して防御する必要もある。

【００１３】従って、このような機器認証システムにおいては、認証データと証明データとの組数は、現実的な計算機のパワーや時間内においては認証データと証明データの全ての組合せが収集されないだけの莫大な数であることが要求される。

【００１４】

【発明が解決しようとする課題】しかしながら、上述の従来の機器認証システムでは、認証データと証明データとの組数を増やすために認証データのデータ長（ビット長）を大きくしようとすると、それを入力とするデータ変換器１２、２１、暗号器３２、復号器４１の回路規模を大幅に増大しなければならないという問題点がある。

【００１５】具体的には、上記従来の機器認証システムでは、認証データと証明データはそれぞれ３２ビットであるので、これらの組合せは全部で２の３２乗通りである。即ち、伝送路には２の３２乗通りの認証データと証明データとの組合せが出現し得る。この場合、１ｍｓの時間で１つの組を伝送路上に出現させてこれを盗むことが出来るとすると、１週間もしないうちに全ての組を収集できてしまう。また、１時間そこそこで入手出来る組数の１００分の１程度のデータに基づいて正規の被認証装置になりすますことが出来る確率も極めて高い。これでは充分に安全な組数とは言えない。

【００１６】このシステムの安全性を高めるためには、例えば認証データを６４ビットに増やすことで上記組数を増加させればよい。しかし、そのためには少なくとも両装置が備えるデータ変換器１２、２１、暗号器３２、復号器４１の回路規模を２倍以上にする必要があり、これでは、回路規模の制約が厳しい小型・携帯型の電子機器や高速な認証手続が要求される通信機器等においては実装が困難であり、断念せざるを得ない。

【００１７】そこで、本発明はかかる問題点に鑑みてな

されたものであり、従来とほぼ等しい回路規模で構成されるにも拘わらず従来の２倍長の認証データを用いて認証を行うことができる安全性の高い機器認証システム及びそのための一方向データ変換装置を提供することを目的とする。

【００１８】

【課題を解決するための手段】上記目的を達成するために、認証装置及び被認証装置に用いられる一方向データ変換装置や暗号器・復号器は、通常、入出力データ長がともにｎビットであり、両装置はｎビットの共通鍵を所持して動作していることに着目し、そのような特性を有効利用することで以下の発明を考案した。

【００１９】本発明は、２ｎビットの入力データを意味のないｎビットの出力データに変換する一方向データ変換装置であって、前記入力データをその入力データの相異なる桁位置のｎビットずつに分離することにより、ｎビットの第１分離データとｎビットの第２分離データを生成する分離手段と、前記第１分離データに対して前記第２分離データを鍵とする変換アルゴリズムに基づいて変換することにより、前記出力データを生成するデータ変換手段とを備える。

【００２０】この一方向データ変換装置は、ｎビットデータからｎビットデータに変換する手段（データ変換手段）にビット分離するための簡単な配線等の手段（分離手段）を付加したものである。このような一方向データ変換装置を備える機器認証システムの一形態は、認証装置が、２ｎビットの乱数を生成する乱数発生手段と、その乱数を２個のｎビットの第１及び第２分離データにビット分離する分離手段と、第１分離データに対して第２分離データを鍵として変換するデータ変換手段と、その変換結果ｎビットと被認証装置から返信されてきた証明データｎビットとが一致するか否かを判断する比較手段とを備え、一方、被認証装置が、認証装置が備える分離手段及びデータ変換手段それぞれと同じ機能の分離手段及びデータ変換手段等を備え、認証装置が発生した２ｎビットの乱数（認証データ）からｎビットの証明データを生成し認証装置に返信する、システムである。

【００２１】ここで、データ変換手段自体は一方向性関数に基づく変換手段であってもよい。また、分離手段で生成された第２分離データを鍵としてデータ変換手段に入力する代わりに、予め記憶された秘密鍵をその第２分離データで変更し、その変更結果を鍵としてデータ変換手段に入力することもできる。また、上記一方向データ変換装置を備える機器認証システムの他の形態は、暗号器と復号器とを用いるシステムであって、認証装置は、２ｎビットの乱数を発生する乱数発生手段と、前記乱数をその乱数の相異なる桁位置のｎビットずつに分離することにより、ｎビットの第１分離データとｎビットの第２分離データを生成する分離手段と、前記第１分離データに対して前記第２分離データを暗号鍵とする暗号アルゴリズムに基づいて暗号化することにより、ｎビットの暗号文を生成する暗号化手段と、前記暗号文と前記第２分離データとを各ビットを混ぜることで結合し、２ｎビットの出力データを生成する結合手段と、前記認証データに対して被認証装置から返信されてきたｎビットの証明データと前記第１分離データとが一致するか否かを判断する比較手段とを備え、一方、被認証装置は、認証装置から送信されてきた認証データをその認証データの相異なる桁位置のｎビットずつに分離することにより、前記暗号文と同じｎビットの第３分離データと前記第２分離データと同じｎビットの第４分離データを生成する分離手段と、前記第３分離データに対して前記第４分離データを復号鍵とする復号アルゴリズムに基づいて復号化することにより、認証装置に返信すべきｎビットの証明データを生成する復号化手段とを備える。

【００２２】ここで、上記第２分離データ（及び第４分離データ）を暗号鍵（復号鍵）として暗号器（復号器）に入力する代わりに、予め記憶された秘密鍵をその第２分離データ（及び第４分離データ）で変更し、その変更結果を暗号鍵（復号鍵）として暗号器（復号器）に入力することもできる。

【００２３】

【発明の実施の形態】以下、本発明に係る機器認証システムについて図面を用いて詳細に説明する。

（実施の形態１）図１は、本発明に係る実施形態１の機器認証システムの構成を示すブロック図である。

【００２４】本システムは、一方向データ変換装置を用いた機器認証システムであり、伝送路６８、６９で接続された認証装置５０と被認証装置６０から構成される。認証装置５０は、被認証装置６０を認証する側の機器であり、乱数発生部５１、一方向データ変換装置５７（分離部５２及びデータ変換器５３）、比較部５４、送信部５５及び受信部５６を備える。

【００２５】乱数発生部５１は、認証に際して１個の並列６４ビットの乱数を発生する。送信部５５は、並列to直列変換器等であり、乱数発生部５１が発生した並列６４ビットの乱数を直列に変換し、認証データとして伝送路６８を介して被認証装置６０に送信する。一方向データ変換装置５７は、６４ビットの入力データを秘密の変換アルゴリズムに基づいて３２ビットの出力データに変換する回路であり、この回路の秘密性を確保するために１個のシリコン基板にＩＣとして形成されており、分離部５２とデータ変換器５３とから構成される。

【００２６】ここで、一方向データ変換装置とは、任意の入力データを変換して１つの出力データを生成するが、生成された出力データからは入力データを一義的に特定できないような変換を行う装置をいう。この一方向データ変換装置５７は、入力データよりも少ないビット数の出力データを生成するので、一方向性の変換を行う装置と言える。

【００２７】分離部５２は、図２に示されるような固定的な配線であり、乱数発生部５１が発生した６４ビットの乱数Ａ０～Ａ６３を、不規則なビット配分に従って、２つの３２ビットの分離データ（Ｂ０～Ｂ３１とＣ０～Ｃ３１）に分離する。つまり、これら２つの分離データは、入力された６４ビットの乱数の相異なる３２個の桁から構成される。

【００２８】データ変換器５３は、分離部５２で生成された１つの３２ビットの分離データＣ０～Ｃ３１を変換対象とし、もう１つの分離データＢ０～Ｂ３１を鍵とする変換関数Ｆ（）に基づいて変換することにより、意味のない３２ビットのデータを生成する論理回路である。受信部５６は、直列to並列変換器等であり、送信部５５が送信した認証データに対して被認証装置６０から返信されてくる直列３２ビットの証明データを受信し、並列に変換して比較部５４に送る。

【００２９】比較部５４は、ラッチ回路及びコンパレータ回路等であり、データ変換器５３が生成した３２ビットのデータと受信部５６から送られてきた３２ビットの証明データとを比較し、それらが一致するか否か判断する。一致した場合は、認証装置５０は被認証装置６０を認証し、そうでない場合は認証しない。一方、被認証装置６０は、認証装置５０に対して自己の正当性を証明する機器であり、一方向データ変換装置６５（分離部６１及びデータ変換器６２）、受信部６３及び送信部６４を備える。

【００３０】受信部６３は、直列to並列変換器等であり、認証装置５０から送信されてきた直列６４ビットの認証データを受信し、並列に変換して分離部６１に送る。一方向データ変換装置６５は、認証装置５０が備える一方向データ変換装置５７と同一であり、６４ビットの入力データを秘密の変換アルゴリズムに基づいて３２ビットの出力データに変換する回路であり、この回路の秘密性を確保するために１個のシリコン基板にＩＣとして形成されており、分離部６１とデータ変換器６２とから構成される。

【００３１】分離部６１は、認証装置５０が備える分離部５２と同一であり、受信部６３から送られてきた６４ビットの認証データＡ０～Ａ６３を２つの３２ビットの分離データ（Ｂ０～Ｂ３１とＣ０～Ｃ３１）に分離する。データ変換器６２は、認証装置５０が備えるデータ変換器５３と同一であり、分離部６１で生成された１つの３２ビットの分離データＣ０～Ｃ３１を変換対象とし、もう１つの分離データＢ０～Ｂ３１を鍵とする変換関数Ｆ（）に基づいて変換することにより、意味のない３２ビットのデータを生成する論理回路である。

【００３２】送信部６４は、並列to直列変換器等であり、データ変換器６２が生成した並列３２ビットのデータを直列に変換し、証明データとして伝送路６９を介して認証装置５０に返信する。図３は、データ変換器５３（及びデータ変換器６２）の詳細な構成を示すブロック図である。

【００３３】このデータ変換器５３（及びデータ変換器６２）は、ビット置換部７０、換字部７１、排他的論理和部７２、転字部７３及びビット置換部７４から構成される。ビット置換部７０は、ラッチ回路及び配線等からなり、入力された３２ビットデータＣ０～Ｃ３１をビット単位で不規則に並び替える。

【００３４】換字部７１は、換字表を記憶するＲＯＭ等からなり、ビット置換部７０から出力された３２ビットデータを４文字からなる文字列（先頭から８ビットずつを１文字とする）として１文字ずつ換字表を引くことで新たな４文字からなる文字列に変換する。排他的論理和部７２は、図４に示されるように３２個のＥＸＯＲゲートからなり、換字部７１から出力された３２ビットデータＤ０～Ｄ３１と分離部５２（分離部６１）から生成された分離データＢ０～Ｂ３１とのビット毎の排他的論理和をとる。

【００３５】転字部７３は、ラッチ回路及び配線等からなり、排他的論理和部７２から出力された３２ビットデータＥ０～Ｅ３１を８ビット×４文字の文字列として、文字の順番を入れ替える。ビット置換部７４は、ラッチ回路及び配線等からなり、転字部７３から出力された３２ビットデータをビット単位で並び替える。この並び替えは、上記ビット置換部７０及び転字部７３のものと異なる。

【００３６】このように、データ変換器５３（及びデータ変換器６２）は、３２ビットの入力データＣ０～Ｃ３１を意味のない３２ビットの出力データに変換するが、そのときの変換アルゴリズムは排他的論理和部７２に入力される分離データＢ０～Ｂ３１の影響を受ける。以上のように構成された本機器認証システムにおける動作は以下の通りである。

【００３７】まず、認証装置５０の乱数発生部５１は、６４ビットの乱数を生成する。送信部５５はその６４ビットの乱数を認証データとして被認証装置６０に送信する。そして、認証装置５０においては、分離部５２は、その６４ビットの乱数を２つの３２ビットの分離データに分離し、データ変換器５３は、一方の分離データに対して他方の分離データを鍵として変換する。

【００３８】一方、被認証装置６０においても、認証装置５０と同様にして、分離部６１は、認証装置５０から受信部６３を経て送られてきた６４ビットの認証データを２つの３２ビットの分離データに分離し、データ変換器６２は、一方の分離データに対して他方の分離データを鍵として変換し、送信部６４を経て認証装置５０に返信する。

【００３９】最後に、認証装置５０の比較部５４は、両装置５０、６０でのデータ変換器５３、６２から出力された２つの３２ビットデータを比較する。その結果、一

致した場合には、認証装置５０は、被認証装置６０が正当な機器であることを認証する。以上のように、本機器認証システムによれば、認証装置５０から被認証装置６０に送られる認証データは、図１５に示された従来システムにおける認証データの２倍長、即ち、６４ビット長であるので、認証データとそれに対応する証明データとの組数は２の６４乗通りとなる。即ち、本システムでは、伝送路に出現し得る認証データと証明データとの総組数は、従来システムにおける組数（２の３２乗通り）の２の３２乗倍となり、不正な第３者による伝送路の盗聴に対する安全性が極めて高くなる。

【００４０】ところで、本機器認証システムに必要とされるハードウェア規模は、第１の従来技術とほとんど変わらない。図１５と図１をに比較して分かるように、本機器認証システムの構成が従来システムと異なる主要な点は、(i)分離部５２（６１）が追加されていることと、(ii)データ変換器５３（６２）が鍵の入力ポートを備えたことである。ここで、(i)分離部５２は単なる固定的な配線によって実現されており、そして、(ii)図３に示されたデータ変換器５３（６２）の構成要素のうち排他的論理和部７２を除く構成要素７０、７１、７３、７４は、３２ビットの入力データを３２ビットの出力データに変換する従来システムのデータ変換器１２（２１）に相当すると言える。

【００４１】従って、本実施形態の機器認証システムは、従来システムとほぼ等しい回路規模で構成されるにも拘わらず従来の２倍長の認証データを用いて認証を行うことができる。

（実施の形態２）図５は、本発明に係る実施形態２の機器認証システムの構成を示すブロック図である。

【００４２】本システムは、実施形態１のシステムと同様に、伝送路６８、６９で接続された認証装置８０と被認証装置９０から構成される。なお、実施形態１と同じ構成要素には同じ符号を付し、その説明は省略する。本実施形態の認証装置８０及び被認証装置９０が実施形態１のものと異なる点は、それぞれが備える一方向データ変換装置８３及び一方向データ変換装置９３の構成要素である。

【００４３】認証装置８０が備える一方向データ変換装置８３は、内部回路の秘密性を確保するために１個のシリコン基板にＩＣとして形成されている点で実施形態１と同じであるが、実施形態１の分離部５２及びデータ変換器５３に加えて、さらに秘密鍵変更部８１と秘密鍵記憶部８２とを備える。秘密鍵記憶部８２は、ＲＯＭ等であり、１個の３２ビットの秘密鍵を記憶している。

【００４４】秘密鍵変更部８１は、図６に示されるように３２個のＥＸＯＲゲートからなり、秘密鍵記憶部８２から読み出した３２ビットの秘密鍵と分離部５２から生成された分離データＢ0～Ｂ31とのビット毎の排他的論理和をとり、得られた３２ビットデータを鍵としてデータ変換器５３に出力する。つまり、実施形態１の一方向データ変換装置５７では、分離部５２から生成された分離データＢ0～Ｂ31は鍵として直接にデータ変換器５３に入力されたが、本実施形態の一方向データ変換装置８３では、分離部５２から生成された分離データＢ0～Ｂ31は秘密鍵記憶部８２に記憶された秘密鍵を変更する目的（又は、秘密鍵記憶部８２に記憶された秘密鍵によって変更される目的）に用いられ、変更された秘密鍵がデータ変換器５３に鍵として入力される。

【００４５】一方、被認証装置９０が備える一方向データ変換装置９３も、認証装置８０の一方向データ変換装置８３と同様に、１個のシリコン基板にＩＣとして形成されており、実施形態１の分離部６１及びデータ変換器６２に加えて、さらに秘密鍵変更部９１と秘密鍵記憶部９２とから構成される。秘密鍵記憶部９２は、認証装置８０の秘密鍵記憶部８２と同一であり、秘密鍵変更部９１は、認証装置８０の秘密鍵変更部８１と同一である。

【００４６】以上のように構成された本機器認証システムによれば、実施形態１のシステムと同様に、従来システムとほぼ等しい回路規模で構成されるにも拘わらず従来の２倍長の認証データを用いて認証を行うことができる。つまり、本実施形態の一方向データ変換装置８３の構成は、従来のデータ変換器１２に分離部５２と秘密鍵変更部８１とを追加した構成に等しいと言える。それは、本実施形態の秘密鍵記憶部８２とデータ変換器５３とからなる回路セット、即ち、固定的な秘密鍵で３２ビットデータを変換する回路セットは、外部からの鍵に依存することなく固定的な変換アルゴリズムに基づいて３２ビットデータを変換する従来システムのデータ変換器１２に相当すると言えるからである。

【００４７】従って、本実施形態の一方向データ変換装置８３は、従来のデータ変換器１２に対して、単なる固定的な配線である分離部５２と３２個のＥＸＯＲゲートからなる秘密鍵変更部８１という、わずかな回路が追加されているに過ぎないと言える。このことは、被認証装置９０が備える一方向データ変換装置９３についても同様である。

【００４８】但し、実施形態１と比較し、本実施形態の機器認証システムは、分離部５２（６１）で生成された分離データが直接ではなく変化を受けた後にデータ変換器５３（６２）への鍵として入力されているので、その変化分だけ安全性は高くなっている。なお、上記実施形態１、２では、一方向データ変換装置５７、６５、８３、９７は６４ビットの入力データに対してビット分離をした後にビット置換等の変換アルゴリズムに基づいて３２ビットの出力データを生成したが、本発明はこのようなビット数や変換アルゴリズムに限定されるものではない。

【００４９】例えば、１２０ビットの入力データを５６ビットの分離データと６４ビットの分離データに分離

し、５６ビットの分離データを暗号鍵として６４ビットの分離データを一般暗号化規格（ＤＥＳ）に従って暗号化してもよい。また、上記実施形態１、２では、データ変換器５３、６２自体は、可逆な変換器（出力データと鍵とから元の入力データに復元する逆変換が存在するような変換をする変換器）であったが、一方向性変換器（出力データと鍵とから元の入力データに復元する逆変換が存在しないような不可逆な変換をする変換器）であってもよい。

【００５０】例えば、データ変換器５３（６２）の排他的論理和部７２を構成する３２個のＥＸＯＲゲートのうち少なくとも１個をＡＮＤゲート又はＯＲゲートに置き換えることによって、そのデータ変換器５３（６２）は一方向性変換器となるが、そのような構成であっても、機器認証システムとして成立する。上記実施形態１、２では、データ変換器５３及び６２は、いずれも同じ方向の変換（２つの分離データから出力データを生成する変換）にのみ用いられているので、逆変換が存在する必要がないからである。

（実施の形態３）図７は、本発明に係る実施形態３の機器認証システムの構成を示すブロック図である。

【００５１】本システムは、第２の従来技術の如く、暗号器と復号器の対を用いた機器認証システムであり、かつ、実施形態２の変形例であり、伝送路６８、６９で接続された認証装置１８０と被認証装置１９０から構成される。なお、実施形態２と同じ構成要素には同じ符号を付し、その説明は省略する。本実施形態の認証装置１８０の構成が実施形態２の認証装置８０と異なる点は、実施形態２の認証装置８０が備える構成要素５１、８３、５４～５６に加えて、さらに結合部１８１を備えることである。なお、データ変換器５３は、実施形態２のものと同一であるが、本実施形態では、暗号器（その逆変換である復号器が存在し、かつ、本機器認証システム（被認証装置１９０）で用いられている）として用いている。

【００５２】結合部１８１は、図８に示されるような固定的な配線であり、分離部５２から秘密鍵変更部８１に入力された３２ビットの分離データＢ０～Ｂ３１と、データ変換器５３が出力した３２ビットデータ（暗号文Ｘ０～Ｘ３１）とを、不規則に各ビットを混ぜて並べることにより、１個の６４ビットデータ（認証データＹ０～Ｙ６３）に結合し送信部５５に送る。この結合部１８１は、秘密性を確保するために、一方向データ変換装置８３の構成要素５２、５３、８１、８２と共に１個のシリコン基板にＩＣとして形成されている。

【００５３】一方、被認証装置１９０は、一方向データ変換装置１９３、受信部６３及び送信部６４を備える点で実施形態２と同じであるが、一方向データ変換装置１９３の構成要素が異なる。つまり、一方向データ変換装置１９３は、１個のシリコン基板にＩＣとして形成された秘密鍵変更部９１、秘密鍵記憶部９２、分離部１９１及びデータ逆変換器１９２から構成されるが、これらのうち、分離部１９１とデータ逆変換器１９２は本実施形態に固有のものである。

【００５４】分離部１９１は、図９に示されるような固定的な配線であり、受信部６３から送られてくる６４ビットの認証データＹ０～Ｙ６３を、認証装置１８０が備える結合部１８１によるビット結合の逆変換に相当するビット配分に従って、元の３２ビットの暗号文Ｘ０～Ｘ３１と３２ビットの分離データＢ０～Ｂ３１とに分離する。データ逆変換器１９２は、認証装置１８０が備えるデータ変換器（暗号器）５３に対応する復号器であり、分離部１９１で生成された３２ビットの暗号文Ｘ０～Ｘ３１を変換対象とし、もう１つの分離データＢ０～Ｂ３１を鍵とする逆変換関数Ｆ-１０に基づいて変換することにより、元の３２ビットの分離データＣ０～Ｃ３１に復号する。

【００５５】図１０は、データ逆変換器１９２の詳細な構成を示すブロック図である。データ逆変換器１９２は、ビット置換部１９９、転字部１９８、排他的論理和部１９７、換字部１９６及びビット置換部１９５から構成され、これらは、それぞれ、図３に示されたデータ変換器５３のビット置換部７４、転字部７３、排他的論理和部７２、換字部７１、ビット置換部７０の逆変換を行うものに等しい。なお、排他的論理和部１９７は、ＥＸＯＲゲート自体の性質より、排他的論理和部７２と同一の構成（３２個のＥＸＯＲゲート）を備える。

【００５６】以上の構成によれば、結合部１８１と分離部１９１、データ変換器５３とデータ逆変換器１９２は、それぞれ逆変換の関係にあり、かつ、秘密鍵記憶部８２と秘密鍵記憶部９２、秘密鍵変更部８１と秘密鍵変更部９１は、それぞれ同一である。従って、データ逆変換器１９２に入力される暗号文はデータ変換器５３が出力した暗号文に等しく、かつ、データ逆変換器１９２に入力される鍵はデータ変換器５３に入力された鍵に等しいことから、データ逆変換器１９２が出力する復号文はデータ変換器５３に入力された平文、即ち、分離部５２が生成した３２ビットの分離データＣ０～Ｃ３１に等しくなる。

【００５７】よって、認証装置１８０の比較部５４は、乱数発生部５１が発生した１個の乱数について分離部５２から入力される分離データと、その乱数に基づいて生成された認証データに対して被認証装置１９０から返信されたきた証明データとが一致すると判定するので、認証装置１８０は被認証装置１９０を認証することができる。

【００５８】以上のように、本機器認証システムと図１６に示された第２の従来技術とを比較して分かるように、本機器認証システムによれば、わずかなハードウェア（分離部５２、１９１、秘密鍵変更部８１、９１、結合部１８１等）を追加しただけで、伝送路６８、６９に

出現し得る認証データを証明データとの総組数は２の６４乗通り、すなわち従来の２の３２乗倍に増加している。つまり、多くの回路を必要とする暗号器及び復号器は従来と同じ３２ビット対応を使用しているにも拘わらず、従来よりも第３者の盗聴に対する安全性は飛躍的に向上されている。

【００５９】なお、本実施形態では、暗号器５３は、実施形態２のデータ変換器５３と同一であったが、本発明はこれに限定されない。暗号器５３としてＤＥＳに準拠した暗号器を用い、復号器１９２として対応する復号器を用いてもよい。また、本実施形態は実施形態２の一方向データ変換装置を用いたシステムを暗号器と復号器とを用いるシステムに変形した例であったが、実施形態１を同様に変形することもできる。つまり、認証装置１８０においては、分離部５２からの分離データＢ０～Ｂ３１を直接に暗号鍵５３の暗号鍵として入力し、一方、被認証装置１９０においても、分離部１９１からの分離データＢ０～Ｂ３１を直接に復号器１９２の復号鍵として入力してもよい。

【００６０】さらに、上記実施形態１～３では、ほとんどの構成要素は論理回路で実現されたが、汎用のマイクロプロセッサとプログラムとの組み合わせによるソフトウェアで実現することも可能である。その場合の「回路規模」とは、そのソフトウェアのコードサイズや、それを収納するＰＲＯＭの記憶容量を意味する。（具体的な通信システムへの適応例）以上のように、本発明に係る機器認証システムは、回路規模が小さいにも拘らず大きなサイズの認証データを扱うことができる。従って、本機器認証システムは、小型で、かつ、正当な機器同士での通信のみが許可されるような高い安全性の要求される通信システムに好適である。

【００６１】図１１は、本発明に係る機器認証システムの具体的な通信システムへの適用例を示す図であり、映画等のデジタル著作物の映像再生システムの概観を示す。このシステムは、認証装置である光ディスクドライブ装置１１０と被認証装置である映像再生装置１１１とそれらを接続するＳＣＳＩケーブル１１６等からなる。光ディスクドライブ装置１１０は、映像再生装置１１１を認証した後に、光ディスク１１５から読み出した映像データを映像再生装置１１１に転送し、そこで映像再生するシステムである。

【００６２】図１２は、光ディスクドライブ装置１１０の構成を示すブロック図である。光ディスクドライブ装置１１０は、装置全体の制御を行うＭＰＵ１２４と、映像再生装置１１１との通信インタフェースであるＳＣＳＩコントローラ１２１と、光ヘッド１２５を制御して光ディスク１１５から映像データを読み出し制御する読み出し制御部１２２と、上述の実施形態における一方向データ変換装置５７、８３、結合部１８１等を内蔵する暗号化ＩＣ１２３とからなり、映像再生装置１１１は正当な機器であると認証した場合にのみ光ディスク１１５に記録された圧縮映像データを読み出してＳＣＳＩケーブル１１６を介して映像再生装置１１１に転送する。

【００６３】図１３は、光ディスクドライブ装置１１０の内部に実装される回路基板１２０の概観を示す図である。暗号化ＩＣ１２３は、１個のシリコン基板に形成されたＬＳＩであり、プラスチックでモールドされたフラットパッケージの形状をしている。図１４は、映像再生装置１１１の構成を示すブロック図である。

【００６４】映像再生装置１１１は、装置全体の制御を行うＭＰＵ１３１と、光ディスクドライブ装置１１０との通信インタフェースであるＳＣＳＩコントローラ１３０と、上述の実施形態の一方向データ変換装置６５、９３、１９３等を内蔵する暗号化ＩＣ１３２と、受信した映像データの伸長を行うＭＰＥＧデコーダ１３３と、伸長された映像データをアナログ映像信号に変換してＣＲＴ１１２及びスピーカ１１４に映像出力するＡＶ信号処理部１３４とから構成される。

【００６５】光ディスクドライブ装置１１０の内部に実装される回路基板の概観は、図１３に示されるものとほぼ同様である。本発明に係る機器認証システムをこのような映像再生システムに適用することで、コンパクトな回路であるのにも拘らず、光ディスク１１５に記録されたデジタル著作物が不正な装置によってコピー等されることが従来よりも極めて困難となり、デジタル著作物の著作権がより強力に保護される。

【００６６】

【発明の効果】以上の説明から明らかなように、本発明に係る一方向データ変換装置は、２ｎビットの入力データを意味のないｎビットの出力データに変換する一方向データ変換装置であって、前記入力データをその入力データの相異なる桁位置のｎビットずつに分離することにより、ｎビットの第１分離データとｎビットの第２分離データを生成する分離手段と、前記第１分離データに対して前記第２分離データを鍵とする変換アルゴリズムに基づいて変換することにより、前記出力データを生成するデータ変換手段とを備える。

【００６７】この一方向データ変換装置は、ｎビットデータからｎビットデータに変換する手段（データ変換手段）にビット分離するための簡単な配線等の手段（分離手段）を付加したものである。従って、このような一方向データ変換装置を認証装置及び被認証装置それぞれが備えることで、従来とほぼ等しい回路規模で構成されるにも拘わらず従来の２倍長の認証データを用いて認証を行うことができる安全性の高い機器認証システムが実現される。

【００６８】つまり、ｎビットの認証データ及び証明データを用いて認証する従来の機器認証システムの構成に対してわずかなハードウェアを追加するだけで、２ｎビットの認証データとｎビットの証明データとを用いて認

証する機器認証システム、即ち、認証データと証明データのとり得る組数が2のn乗通りから2の2n乗通り（2のn乗倍）に増加された安全性の高い機器認証システムが実現される。

【0069】このような一方向データ変換装置を備える機器認証システムの一形態は、認証装置が、2nビットの乱数を生成する乱数発生手段と、その乱数を2個のnビットの第1及び第2分離データにビット分離する分離手段と、第1分離データに対して第2分離データを鍵として変換するデータ変換手段と、その変換結果nビットと被認証装置から返信されてきた証明データnビットとが一致するか否かを判断する比較手段とを備え、一方、被認証装置が、認証装置が備える分離手段及びデータ変換手段それぞれと同じ機能の分離手段及びデータ変換器手段等を備え、認証装置が発生した2nビットの乱数（認証データ）からnビットの証明データを生成し認証装置に返信する、システムである。

【0070】ここで、データ変換手段自体は一方向性関数に基づく変換手段であってもよい。また、分離手段で生成された第2分離データを鍵としてデータ変換手段に入力する代わりに、予め記憶された秘密鍵をその第2分離データで変更し、その変更結果を鍵としてデータ変換手段に入力することもできる。これによって、データ変換手段自体の解読が困難となり、また、一方向データ変換装置のアルゴリズムが複雑化されるので、システムの安全性はさらに高まる。

【0071】また、上記一方向データ変換装置を備える機器認証システムの他の形態は、暗号器と復号器とを用いるシステムであって、認証装置は、2nビットの乱数を発生する乱数発生手段と、前記乱数をその乱数の相異なる桁位置のnビットずつに分離することにより、nビットの第1分離データとnビットの第2分離データを生成する分離手段と、前記第1分離データに対して前記第2分離データを暗号鍵とする暗号アルゴリズムに基づいて暗号化することにより、nビットの暗号文を生成する暗号化手段と、前記暗号文と前記第2分離データとを各ビットを混ぜることで結合し、2nビットの出力データを生成する結合手段と、前記認証データに対して被認証装置から返信されてきたnビットの証明データと前記第1分離データとが一致するか否かを判断する比較手段とを備え、一方、被認証装置は、認証装置から送信されてきた認証データをその認証データの相異なる桁位置のnビットずつに分離することにより、前記暗号文と同じnビットの第3分離データと前記第2分離データと同じnビットの第4分離データを生成する分離手段と、前記第3分離データに対して前記第4分離データを復号鍵とする復号アルゴリズムに基づいて復号化することにより、認証装置に返信すべきnビットの証明データを生成する復号化手段とを備える。

【0072】ここで、上記第2分離データ（及び第4分離データ）を暗号鍵（復号鍵）として暗号器（復号器）に入力する代わりに、予め記憶された秘密鍵をその第2分離データ（及び第4分離データ）で変更し、その変更結果を暗号鍵（復号鍵）として暗号器（復号器）に入力することもできる。これによって、基本的な構成要素はnビット対応の回路規模であるにも拘らず、即ち、認証装置及び被認証装置それぞれはnビット対応の暗号器及び復号器を備えるにも拘らず、2nビットの認証データとnビットの証明データを扱う安全性の高い機器認証システムが実現される。

【0073】以上のように、本発明によって、認証に用いる一方向データ変換装置や暗号器・復号器の規模をほとんど増大させることなく、認証データと証明データの総組数は2のn乗倍に増大するため、毎回の認証時に伝送路に出現する変換前後の伝送データを不正な第3者が1組ずつ観測して収集することで全ての組について知り尽くすことが極めて困難となり不正な認証が防止される。

【0074】よって、本発明により、わずかなハードウェアを追加するだけで、極めて解読が困難で安全性の高い認証システムが構築され、その実用性は大きい。

【図面の簡単な説明】

【図1】本発明に係る実施形態1の機器認証システムの構成を示すブロック図である。

【図2】同機器認証システムの分離部52（61）の詳細な構成を示す図である。

【図3】同機器認証システムのデータ変換器53（及びデータ変換器62）の詳細な構成を示すブロック図である。

【図4】同データ変換器53（62）の排他的論理和部72の詳細な構成を示す図である。

【図5】本発明に係る実施形態2の機器認証システムの構成を示すブロック図である。

【図6】同機器認証システムの秘密鍵変更部81（91）の詳細な構成を示す図である。

【図7】本発明に係る実施形態3の機器認証システムの構成を示すブロック図である。

【図8】同機器認証システムの結合部181の詳細な構成を示す図である。

【図9】同機器認証システムの分離部191の詳細な構成を示す図である。

【図10】同機器認証システムのデータ逆変換器192の詳細な構成を示すブロック図である。

【図11】本発明に係る機器認証システムの具体的な通信システムへの適用例を示す図である。

【図12】同通信システムにおける光ディスクドライブ装置110（認証装置）の構成を示すブロック図である。

【図13】同光ディスクドライブ装置110の内部に実装される回路基板120の概観を示す図である。

21

【図１４】同通信システムにおける映像再生装置１１１（被認証装置）の構成を示すブロック図である。

【図１５】一方向性関数を用いた第１の従来技術に係る機器認証システムの構成を示すブロック図である。

【図１６】暗号器と復号器の対を用いた第２の従来技術に係る機器認証システムの構成を示すブロック図である。

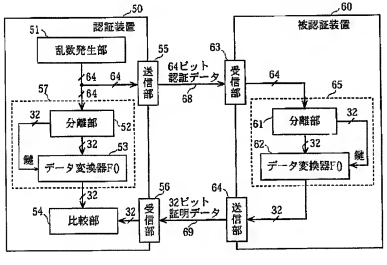
【符号の説明】

５０、８０、１８０　認証装置
５１　乱数発生部
５２　分離部
５３　データ変換器
５４　比較部
５５　送信部
５６　受信部
５７　一方向データ変換装置
６０、９０、１９０　被認証装置

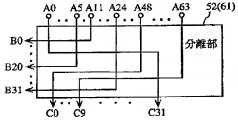
22

６１　分離部
６２　データ変換器
６３　受信部
６４　送信部
６５　一方向データ変換装置
６８　伝送路
６９　伝送路
８１　秘密鍵変更部
８２　秘密鍵記憶部
８３　一方向データ変換装置
９１　秘密鍵変更部
９２　秘密鍵記憶部
９３　一方向データ変換装置
１８１　結合部
１９１　分離部
１９２　データ逆変換器
１９３　一方向データ変換装置

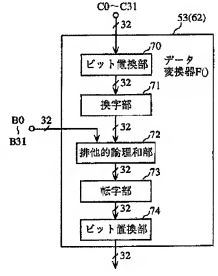
【図１】



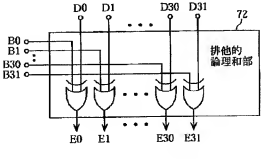
【図２】



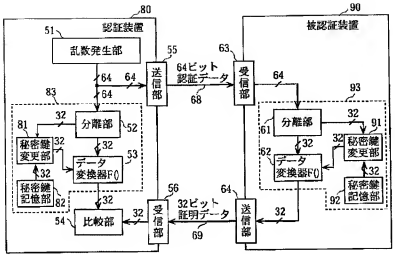
【図３】



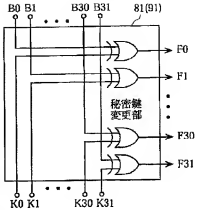
【図４】



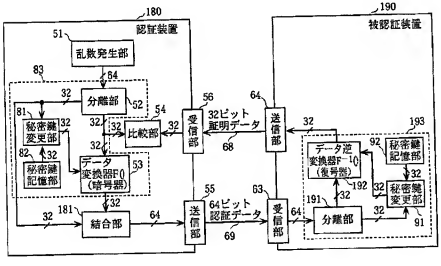
【図５】


80
認証装置
51
乱数発生部
55
送信部
64ビット認証データ
68
受信部
63
90
被認証装置
64
64
83
64
32
分離部
52
81
秘密鍵変更部
32
32
データ変換器F0
53
32
秘密鍵記憶部
82
32
比較部
54
56
受信部
32ビット照明データ
69
送信部
64
32
分離部
32
61
91
秘密鍵変更部
32
32
データ変換器F0
62
32
秘密鍵記憶部
92
93

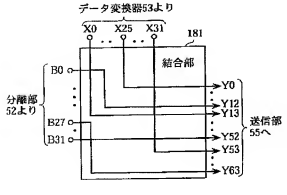
【図６】


B0 B1
B30 B31
81(91)
F0
F1
秘密鍵変更部
F30
F31
K0 K1
K30 K31

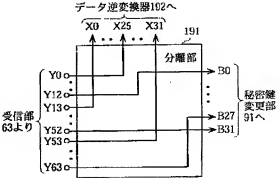
【図７】


180
認証装置
51
乱数発生部
83
64
32
分離部
52
81
秘密鍵変更部
32
32
比較部
32
54
56
受信部
32ビット照明データ
68
送信部
64
32
190
被認証装置
193
データ逆変換器F-1(復号部)
92
秘密鍵記憶部
32
秘密鍵変更部
82
32
秘密鍵記憶部
32
データ変換器F0(暗号部)
53
32
181
結合部
64
送信部
55
64ビット認証データ
69
受信部
63
64
191
分離部
32
91
192
32

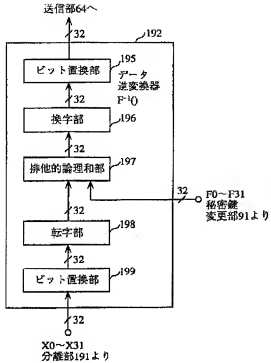
【図８】


データ変換器53より
X0
X25
X31
181
結合部
B0
B27
B31
Y0
Y12
Y13
Y52
Y53
Y63
分離部52より
送信部55へ

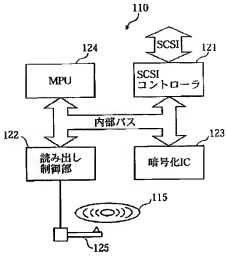
【図９】


データ逆変換器102へ
X0
X25
X31
191
分離部
Y0
Y12
Y13
Y52
Y53
Y63
B0
B27
B31
受信部63より
秘密鍵変更部91へ

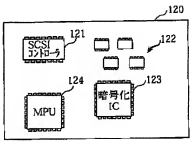
【図１０】



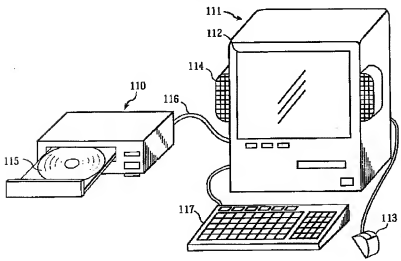
【図１２】



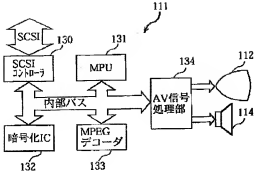
【図１３】



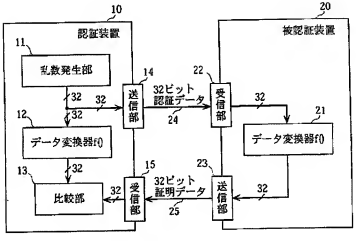
【図１１】



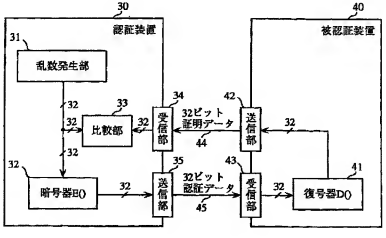
【図１４】


111
SCSI
130
131
SCSI
コントローラ
MPU
134
112
内部バス
AV信号
処理部
114
暗号化IC
MPEG
デコーダ
132
133

【図１５】


10
認証装置
20
被認証装置
11
乱数発生部
14
22
12
データ変換器f()
21
データ変換器f()
13
比較部
15
23
送信部
受信部
32ビット
認証データ
24
32ビット
証明データ
25
32

【図１６】


30
認証装置
40
被認証装置
31
乱数発生部
33
比較部
34
42
32ビット
証明データ
44
35
43
32ビット
認証データ
45
32
暗号器E()
41
復号器D()
送信部
受信部

フロントページの続き

(72)発明者　平山　康一
神奈川県川崎市幸区柳町70番地　株式会社
東芝柳町工場内